

Nilpotency and the number of word maps of a finite group

Alexander Bors*

April 27, 2017

Abstract

For a finite group G and a non-negative integer d , denote by $\Omega_d(G)$ the number of functions $G^d \rightarrow G$ that are induced by substitution into a word with variables among X_1, \dots, X_d . In this note, we show that nilpotency of G can be characterized through the asymptotic growth rate of $\Omega_d(G)$ as $d \rightarrow \infty$.

1 Introduction

1.1 Motivation and main results

In recent years, various authors have made contributions to the theory of word maps on groups; we refer interested readers to the survey article [2] for an overview of results and open problems of this theory.

Recall that a *word* is just an element w of some free group $F(X_1, \dots, X_d)$ and that each such word gives rise to a *word map* $w_G : G^d \rightarrow G$ on every group G , induced by substitution. For a fixed finite group G , denote by $\Omega_d(G)$ the number of functions $G^d \rightarrow G$ that are of the form w_G for some $w \in F(X_1, \dots, X_d)$. Moreover, set $\omega_d := \log_2 \Omega_d(G)$ (binary logarithm). The aim of this note is to show the following:

Theorem 1.1.1. *Let G be a finite group, c a non-negative integer.*

1. *If G is nilpotent of class exactly c , then $\omega_d(G) = \Theta(d^c)$ as $d \rightarrow \infty$.*
2. *If G is not nilpotent, then $\omega_d(G) \geq 2^d - 1$.*

*University of Salzburg, Mathematics Department, Hellbrunner Straße 34, 5020 Salzburg, Austria.
E-mail: alexander.bors@sbg.ac.at

The author is supported by the Austrian Science Fund (FWF): Project F5504-N26, which is a part of the Special Research Program “Quasi-Monte Carlo Methods: Theory and Applications”.

2010 *Mathematics Subject Classification*: Primary: 20D15, 20D60. Secondary: 20E05, 20E10, 20F18.

Key words and phrases: Word map, Finite group, Nilpotent group.

In particular, if G is nilpotent of class c , then for some large enough constant $C = C(G) > 0$, we have $\Omega_d(G) \leq C^{d^c}$ for all non-negative integers d , whereas $\Omega_d(G)$ grows doubly exponentially in d if G is not nilpotent. Note that the trivial upper bound $\Omega_d(G) \leq |G|^{|G|^d}$ is also doubly exponential in d for fixed G . By Theorem 1.1.1, we also have the following quantitative characterization of nilpotency of finite groups:

Corollary 1.1.2. *A finite group G is nilpotent (of class exactly c) if and only if the sequence $(\omega_d(G))_{d \geq 0}$ is of polynomial growth (of degree exactly c).*

1.2 Notation

We denote by \mathbb{N} the set of natural numbers (including 0) and by \mathbb{N}^+ the set of positive integers. The set of all *nonempty* subsets of a set X is denoted by $\mathcal{P}_{\neq \emptyset}(X)$. The exponent of a finite group G is denoted by $\exp(G)$. As in the previous subsection, we denote by $F(X_1, \dots, X_d)$ the free group on the formal generators X_1, \dots, X_d , and we will denote by $F_c(X_1, \dots, X_d)$ the free nilpotent group of class exactly c on the formal generators X_1, \dots, X_d .

1.3 Normal forms of elements in free nilpotent groups

For the reader's convenience, we briefly recall a result on normal forms of elements in free nilpotent groups (based on a certain polycyclic decomposition of such groups) which we will need, see the blog post [3] or the textbook [1, Theorem 5.13A, p. 343, and its proof] for more details.

Fix $d, c \in \mathbb{N}$, and assign to each $i \in \{1, \dots, d\}$ the *weight* $\text{wt}(i) := 1$. Consider formal iterated commutators of the numbers $1, \dots, d$ (we will henceforth call them *formal d -commutators*) and define the *weight* of a formal d -commutator recursively via $\text{wt}([\alpha, \beta]) := \text{wt}(\alpha) + \text{wt}(\beta)$. Moreover, for a formal d -commutator γ , define X_γ , a word in the variables X_1, \dots, X_d , recursively via $X_{[\alpha, \beta]} := [X_\alpha, X_\beta] = X_\alpha^{-1} X_\beta^{-1} X_\alpha X_\beta$.

Then there exists an explicitly constructible finite ordered tuple $(\alpha_1^{(d,c)}, \dots, \alpha_{N_{d,c}}^{(d,c)})$ of pairwise distinct formal d -commutators each of weight at most c such that every element of $F_c(X_1, \dots, X_d)$ has a unique representation of the form $\prod_{j=1}^{N_{d,c}} (X_{\alpha_j^{(d,c)}})^{k_j}$ with $k_j \in \mathbb{Z}$.

For later use, we also note the following, which can be easily proved by induction on c :

Lemma 1.3.1. *For each $c \in \mathbb{N}$, there exists a polynomial $P_c(X) \in \mathbb{Z}[X]$ of degree c such that for every $d \in \mathbb{N}$, the number of formal d -commutators of weight at most c is exactly $P_c(d)$. \square*

See also [1, Problems for Section 5.2, Problem 5] for a precise formula for the coefficients of $P_c(d)$.

2 Proof of Theorem 1.1.1

We begin by providing a lower bound on $\Omega_d(G)$ which will yield both statement (2) of Theorem 1.1.1 and half of statement (1). For this, we need some notation.

Notation 2.1. Let G be a group.

1. For $r \in \mathbb{N}^+$ and elements $g_1, \dots, g_r \in G$, we define their nested commutator $[g_1, \dots, g_r]$ recursively via $[g_1] := g_1$ and $[g_1, \dots, g_{r+1}] := [[g_1, \dots, g_r], g_{r+1}]$.
2. If G is finite and $r \in \mathbb{N}^+$, then denote by $\exp_r(G)$ the least common multiple of the orders of the elements of G of the form $[g_1, \dots, g_r]$, where the g_i range over G .

Note that for fixed finite G , the sequence $(\exp_r(G))_{r \geq 1}$ is monotonically decreasing and that $\exp_1(G) = \exp(G)$.

Definition 2.2. Let G be a finite group, $d \in \mathbb{N}$.

1. A function $f : \mathcal{P}_{\neq \emptyset}(\{1, \dots, d\}) \rightarrow \mathbb{N}$ is called G -admissible if and only if for each $r \in \{1, \dots, d\}$, we have $f(M) < \exp_r(G)$ for every r -element subset $M \subseteq \{1, \dots, d\}$.
2. To each G -admissible function f , we assign a word $w_f(X_1, \dots, X_d)$, defined as follows:

$$w_f(X_1, \dots, X_d) := \prod_{r=1}^d \prod_{i_1=1}^d \prod_{i_2=i_1+1}^d \cdots \prod_{i_r=i_{r-1}+1}^d [X_{i_1}, \dots, X_{i_r}]^{f(\{i_1, \dots, i_r\})}.$$

We now show:

Proposition 2.3. Let G be a finite group, $d \in \mathbb{N}$.

1. Let f, g be distinct G -admissible functions $\mathcal{P}_{\neq \emptyset}(\{1, \dots, d\}) \rightarrow \mathbb{N}$. Then the word maps $(w_f)_G$ and $(w_g)_G$ are distinct functions $G^d \rightarrow G$.
2. $\Omega_d(G) \geq \prod_{r=1}^d \exp_r(G)^{\binom{d}{r}}$.

Proof. Statement (2) follows from statement (1), as the asserted lower bound is by definition just the number of G -admissible functions $\mathcal{P}_{\neq \emptyset}(\{1, \dots, d\}) \rightarrow \mathbb{N}$.

As for statement (1), let $r \in \mathbb{N}^+$ be minimal such that f and g disagree on some r -element subset of $\{1, \dots, d\}$ and let $i_1 < i_2 < \dots < i_r$ be such that $\{i_1, \dots, i_r\}$ is minimal with respect to the lexicographical ordering among all r -element subsets of $\{1, \dots, d\}$ on which f and g have different values. Set $a := f(\{i_1, \dots, i_r\}) - g(\{i_1, \dots, i_r\})$ and note that $a \in \{1, \dots, \exp_r(G) - 1\}$. By definition of $\exp_r(G)$, this means that we can fix $g_{i_1}, \dots, g_{i_r} \in G$ such that

$$[g_{i_1}, \dots, g_{i_r}]^{f(\{i_1, \dots, i_r\}) - g(\{i_1, \dots, i_r\})} \neq 1_G.$$

Moreover, set $g_i := 1_G$ for $i \in \{1, \dots, d\} \setminus \{i_1, \dots, i_r\}$.

We claim that $(w_f)_G$ and $(w_g)_G$ disagree on the argument (g_1, \dots, g_d) . To see this, note that by choice of (i_1, \dots, i_r) , we have

$$w_f = w_0 \cdot [X_{i_1}, \dots, X_{i_r}]^{f(\{i_1, \dots, i_r\})} \cdot w_1$$

and

$$w_g = w_0 \cdot [X_{i_1}, \dots, X_{i_r}]^{g(\{i_1, \dots, i_r\})} \cdot w_2,$$

where $w_0, w_1, w_2 \in F(X_1, \dots, X_d)$ and w_1, w_2 are products of nested commutators of length at least r distinct from $[X_{i_1}, \dots, X_{i_r}]$, so that when substituting g_i for X_i , at least one of the entries of each such nested commutator will be 1_G , forcing it to be trivial. Therefore,

$$\begin{aligned} (w_f)_G(g_1, \dots, g_d) &= w_0(g_1, \dots, g_d) \cdot [g_{i_1}, \dots, g_{i_r}]^{f(\{i_1, \dots, i_r\})} \\ &\neq w_0(g_1, \dots, g_d) [g_{i_1}, \dots, g_{i_r}]^{g(\{i_1, \dots, i_r\})} = (w_g)_G(g_1, \dots, g_d), \end{aligned}$$

as required. \square

Corollary 2.4. *Let G be a finite group, $c \in \mathbb{N}$, and assume that the $(c+1)$ -th term in the lower central series of G is nontrivial. Then for every $d \in \mathbb{N}$, $\omega_d(G) \geq \sum_{r=1}^c \binom{d}{r}$.*

Proof. By assumption, $\exp_r(G) \geq 2$ for $r = 1, \dots, c$, so the result follows immediately from Proposition 2.3(2). \square

In particular, $d^c = \mathcal{O}(\omega_d(G))$ whenever G is nilpotent of class exactly c (which is “half of Theorem 1.1.1(1)”) and if G is not nilpotent, we can choose $c := d$ in Corollary 2.4 and get Theorem 1.1.1(2) using that $\sum_{r=1}^d \binom{d}{r} = 2^d - 1$. The second half of Theorem 1.1.1(1) is provided by the following:

Lemma 2.5. *Let $c \in \mathbb{N}$, and let $P_c(X) \in \mathbb{Z}[X]$ be as in Lemma 1.3.1. Then for every finite nilpotent group G of class exactly c , we have $\omega_d(G) \leq P_c(c) \cdot \log_2(\exp(G))$.*

Proof. We show the equivalent $\Omega_d(G) \leq \exp(G)^{P_c(c)}$. Let $w \in F(X_1, \dots, X_d)$. Then the remarks in Subsection 1.3 yield that

$$w_{F_c(X_1, \dots, X_d)}(X_1, \dots, X_d) = \prod_{j=1}^{N_{d,c}} ((X_{\alpha_j^{(d,c)}})^{k_j}).$$

for suitable integers k_j . As $F_c(X_1, \dots, X_d)$ is the free object in the category of nilpotent groups of class at most c , this relation among its generators translates to an identity in all nilpotent groups of class at most c , yielding in particular that $w_G = (\prod_{j=1}^{N_{d,c}} ((X_{\alpha_j^{(d,c)}})^{k_j}))_G$. Hence each word map on G is induced by a word of the form $\prod_{j=1}^{N_{d,c}} ((X_{\alpha_j^{(d,c)}})^{k_j})$ for suitable integers k_j , which we may w.l.o.g. assume to be from the finite range $\{0, \dots, \exp(G) - 1\}$. Therefore, $\Omega_d(G) \leq \exp(G)^{N_{d,c}} \leq \exp(G)^{P_c(c)}$, as required. \square

References

- [1] W. Magnus, A. Karrass and D. Solitar, *Combinatorial Group Theory. Presentations of Groups in Terms of Generators and Relations*, Interscience Publishers (Pure and Applied Mathematics, XIII) (1966).
- [2] A. Shalev, Some results and problems in the theory of word maps, in: *Erdős Centennial*, Budapest, János Bolyai Math. Soc. (Bolyai Soc. Math. Stud., 25) (2013), 611–649.
- [3] T. Tao, The free nilpotent group, blog post (2009), <https://terrytao.wordpress.com/2009/12/21/the-free-nilpotent-group/>.